EXHIBIT A

Excerpts of SW-SEC00043620


USER ACCESS MANAGEMENT
JANUARY 8, 2018
TOOL EVALUATION & RECOMMENDATION

THE PROBLEM

solarwinds

Problem Statement:

- Currently there is a collection of people who have access to many systems and many people involved in provisioning access. It is suspected that without a standardized process including an annual audit, system users who have changed roles or left the company may still have access to critical data.
- ***The lack of standardized user access management processes that captures user provisioning (hiring), user changes (transfer) and user de-provisioning (resignation and termination), across the organization create a loss risk of organizational assets and personal data.***

Problem Discovery Background:

- GDPR calls within Article 32 "Security of Processing, Recital 75 "*In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.*" Access management is a key component to meeting this requirement.
- Under GDPR, SolarWinds has published and circulated Access Control Guidelines (v1.1) to establish a standard and exception process across the organization. As part of this process, it was discovered that there is no organization-wide, standardized approach to access management that includes provisioning, changing and de-provisioning users access to systems that contain personal information.
- Reference: JIRA Task GDPR-835

2

TOOL ANALYSIS

solarwinds

Between November and December 2017, a group of IT Team members reviewed available tools that are currently used for user access management and others that may be used for this purpose.

The following **tools were evaluated**:

- **Azure AD leveraging SharePoint workflow:** Currently using Azure for AD authentication and some users have access to Microsoft O365 (~400). Full roll out expected in 2018.
- **Web Help Desk:** Currently used to track technical issues and some user access requests.
- **Data Subject Right (DSR) Tool:** Currently being built to manage GDPR data subject right requests.
- **OKTA:** Currently used for user access management for certain applications and instances.
- **Thycotic:** Currently using Thycotic Secret Server used for password management for secure systems.

The **evaluation criteria** used for each tool:

Is the tool ***API friendly***?	Does the application have the capability for access/role level, ***audit reporting***?
Does the tool have the capability for ***Identity Management***?	Does the tool have the capability to interact with ***non-AD authentication***?
Does the tool have the capability for ***Role Management***?	If this tool is chosen, will ***internal or external development work*** be needed?
Does the tool have capability for ***permission workflow***?	If this tool is chosen, is there a ***cost for additional licenses***?
Does the tool have the capability to recognize ***privileged access***?	

3

SOLUTION EVALUATION SUMMARY

solarwinds

Requirement (Desired Response) [Points for DR]	API friendly (Y) [2]	Identity Mgmt. (Y) [5]	Role Mgmt. (Y) [5]	Permission Workflow (Y) [5]	Privileged Access (Y) [5]	Audit Reporting (Y) [5]	Non-AD friendly (Y) [3]	Additional License Cost (N) [3]	External Development (Y) [1]	In-house Development (Y) [1]	Total Tool Points	Total Available Points	%
Azure	Y(2)	Y(5)	Y(5)	Y(5)	Y(5)	Y(5)	Y(3)	N(3)	Y(1)	Y(1)	35	35	100%
OKTA	Y (2)	Y (5)	Y (5)	N (0)	Y (5)	Y (5)	Y (3)	N (3)	Y (1)	Y (1)	30	35	86%
Swipe/Gator Tool (Customized Solution)	Y(2)	N(0)	N(0)	Y(5)	N(0)	Y(5)	Y(3)	N(3)	Y(1)	Y(1)	25	35	71%
Thycotic	N(0)	Y(5)	Y(5)	N(0)	Y(5)	Y(5)	Y(3)	Y(0)	Y(1)	Y(1)	25	35	71%
Web Help Desk	N(0)	N(0)	N(0)	N(0)	N(0)	Y(5)	Y(3)	N(3)	N(0)	Y(1)	12	35	34%

4

PROPOSED RECOMMENDATION

solarwinds

Recommended Solution: *Leverage Azure for user access management and incorporate SharePoint workflows for end users and permission management.*

- Azure AD:
  - is an identity and access management solution that provides directory services, identity governance and application access management.
  - enables Single Sign On (SSO) and is pre-integrated with custom and commercial applications.
- Azure Role-Based Access Control (RBAC):
  - provides exact permissions for users based on three basic roles: owner, contributor or reader.
- Microsoft O365 includes SharePoint:
  - Utilize / leverage SharePoint workflow for access request processing and tracking.

Considerations:

Pro	Con
Pre-built templates provided within O365 license.	Workflow configuration would require external resources.
Market has helpdesk, asset management, facilities, contract renewals and onboarding templates/resources (ex. CrowCanyon Software)	New to the organization, requires end user training.
Enables some momentum for rationalization (ex. OKTA, AutoSARF)	

5